APNT CONOPS DOCUMENT FEEDBACK

DEFINING NEXTGEN APNT

RYAN H. WU, JON PARIS
05/03/2012
Saab Sensis Corporation

(FOR FAA APNT INDUSTRY DAY)

RESILIENT PERFORMANCE BASED NAV (R-PBN) FOR NEXTGEN APNT

- ***Currently-available APNT*** is based on DME, VOR, and ILS technologies that partially sustain desired PBN capabilities
- ***NextGen APNT*** is based on DME, ILS, and yet-to-be-defined technologies that fully sustain desired PBN capabilities
- We propose a new terminology, ***Resilient PBN*** *(R-PBN),* for NextGEN APNT to distinguish it from the currently-available DME/VOR/ILS based APNT concept

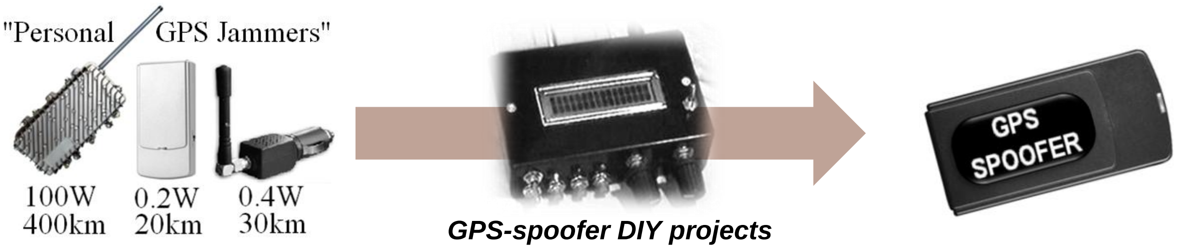
R-PBN DEFINED

R-PBN

- NextGen PBN allows more aircraft to fly from point A to point B in shorter time, with less fuel, and in currently difficult conditions resulting in economic profit and societal benefits
- PBN being dependent on GPS, however, is extremely vulnerable
  - ***GPS jamming, interference, and malfunctions*** deny aircraft access to main navigation signal
  - ***GPS spoofing*** misleads aircraft with false position and false other-ship positions via ADS-B
  - ***ADS-B spoofing*** directly injects false traffic info, confusing pilots, controllers, and advisory and automation systems
  - ***APNT spoofing*** confuses backup navigation systems
- ***Jamming* and *spoofing*** threaten flight safety, disrupt efficiency, reduce capacity, create havoc in the air
  - Economic loss and potential loss of lives
- We need jamming and spoofing ***Resilient PBN*** to ensure NextGen's safety and efficiency

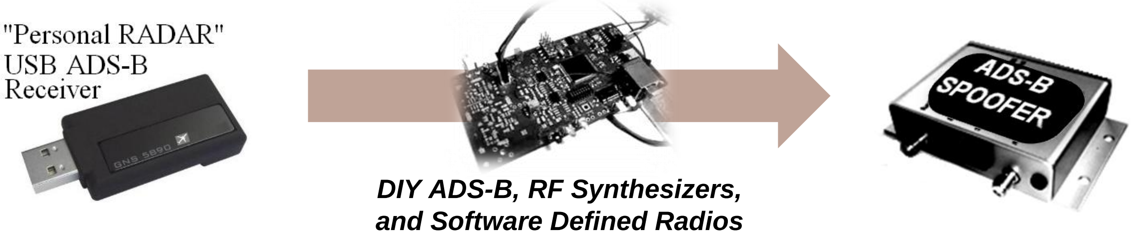
TOMORROW’S THREATS, TODAY’S PLAN

- From today’s cheap “Personal Privacy GPS Jammer” to tomorrow’s cheap “Personal GPS Spoofer” which further falsifies position info for unlawful applications



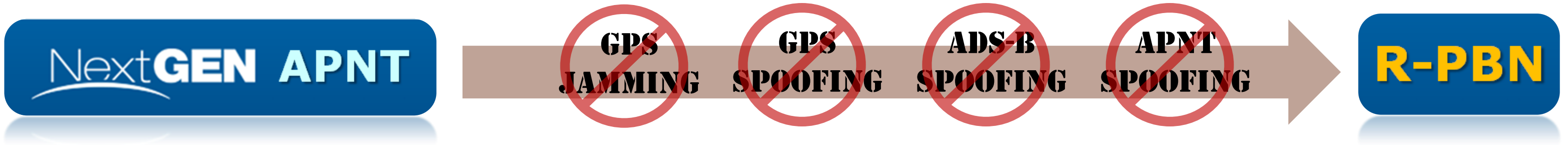
GPS-spoofer DIY projects

- From today’s cheap “Personal ADS-B RADAR” to tomorrow’s low-tech “ADS-B Spoofer” which mimics ADS-B transmissions



DIY ADS-B, RF Synthesizers, and Software Defined Radios

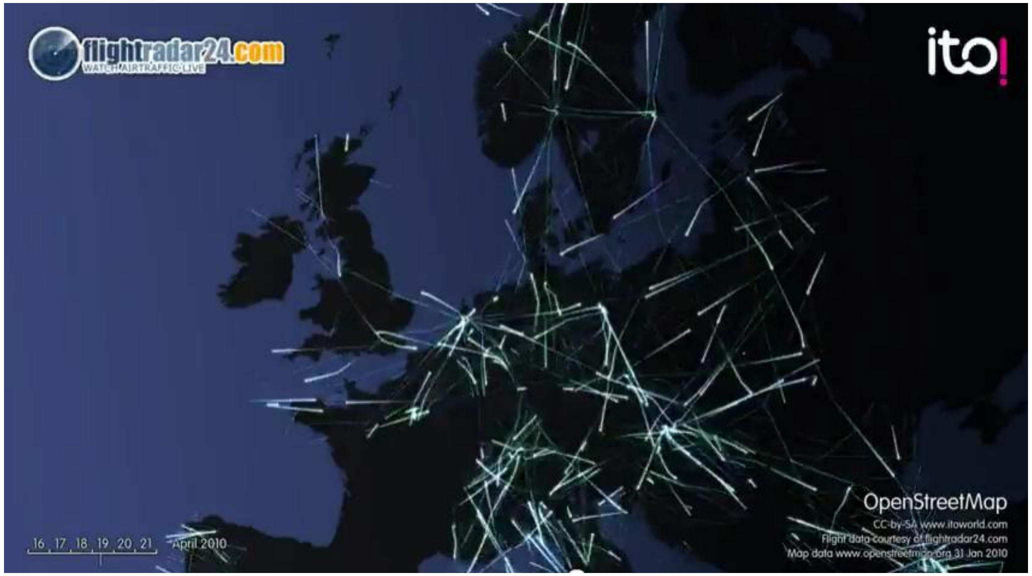
- A more prudent approach to APNT CONOPS may need to consider both ***jamming*** and ***spoofing*** threats



OPEN-ACCESS ADS-B

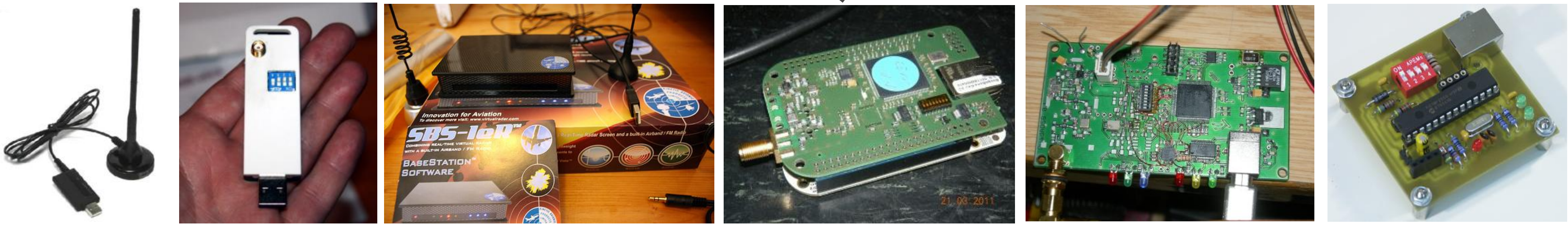
- ADS-B is a great but vulnerable technology
- It allows open **READ** access to everyone
- It cannot deny nor detect unlawful **WRITE** access from anyone
  - An open invitation to spoofers
    - accidental / for fun / criminal
    - malicious / terrorist attack
  - Its impact can be painful
  - From receiving to transmission is just a small step forward!

(please click the image to link to the website for movie)


flightradar24.com
WATCH AIRTRAFFIC LIVE
ito!
OpenStreetMap
CC-by-SA www.itoworld.com
Flight data courtesy of flightradar24.com
Map data www.openstreetmap.org 31 Jan 2010
16 17 18 19 20 21
April 2010

"Transport mapping specialist ITO has compiled the sequence of images, with the aid of real-time flight-monitoring site Flightradar24 which draws data from a network of amateur tracking stations."

"Crowd-sourced" "EURO ADS-B Network"

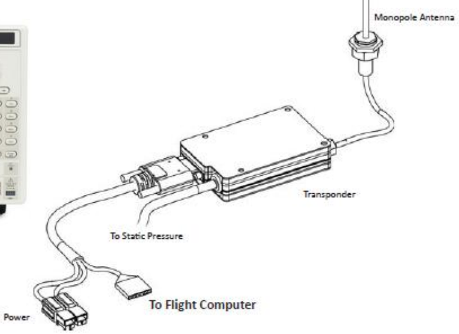


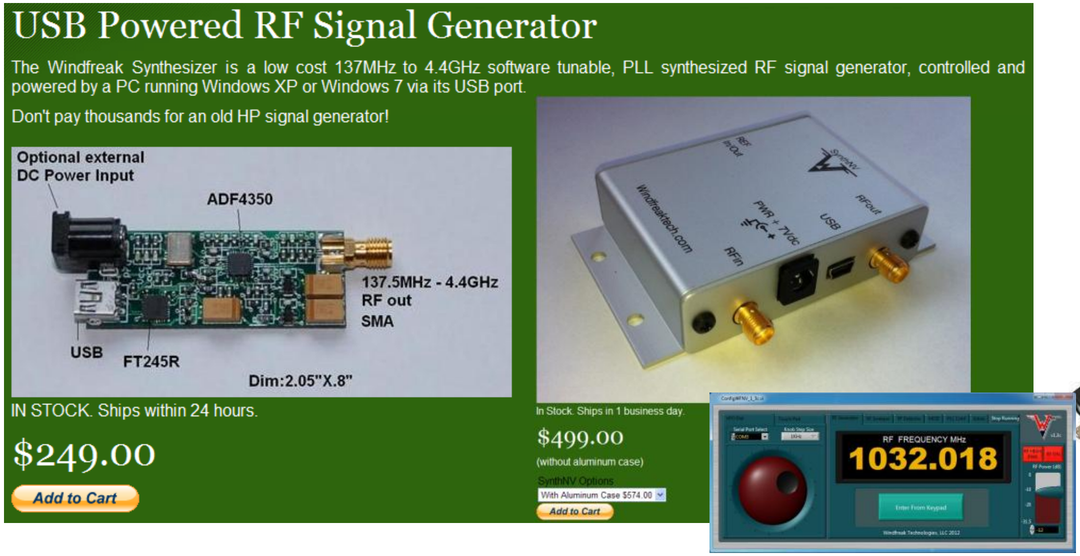
Abundant low-cost Personal ADS-B RADAR Devices and DIY Projects on the Internet

ADS-B SPOOFING IS NOT DIFFICULT

- It’s not difficult to transmit illegitimate ADS-B signals
  - 1090MHz pulsed waveform is extremely simple to create
  - RF Synthesizer
  - Software Defined Radio
  - ADS-B out box fed with fake GPS position data
- Is getting easier and cheaper every year

Sagetech’s Mode S Transponder with ADS-B In/Out (250W)





USB Powered RF Signal Generator

The Windfreak Synthesizer is a low cost 137MHz to 4.4GHz software tunable, PLL synthesized RF signal generator, controlled and powered by a PC running Windows XP or Windows 7 via its USB port.

Don't pay thousands for an old HP signal generator!

IN STOCK. Ships within 24 hours.

$249.00

Add to Cart

In Stock. Ships in 1 business day.

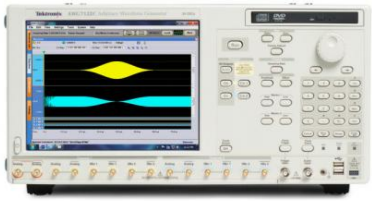
$499.00

(without aluminum case)

SynthNV Options

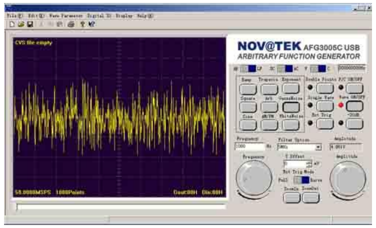
With Aluminum Case $574.00

Add to Cart



$70K Lab AWF

$200 AWF

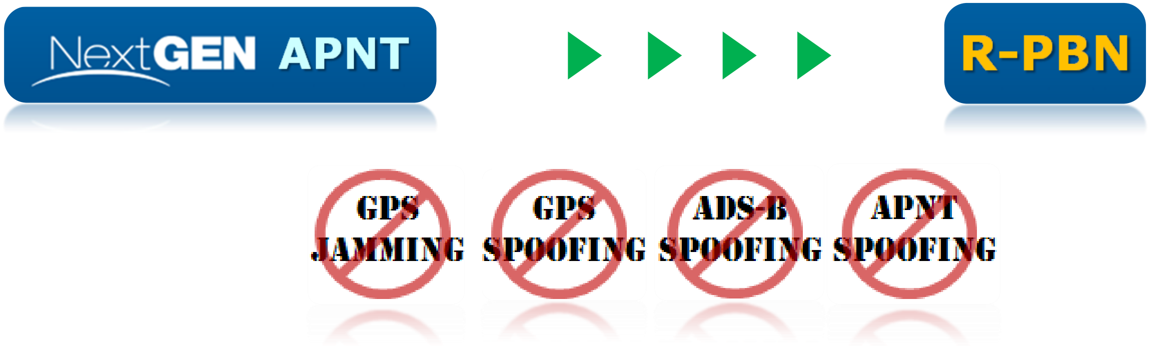


SPOOFING IMPACTS NAVIGATION

- GPS and ADS-B message spoofing can cause great havoc in the air
  - Pilot Confusion
  - Lost of confidence in air traffic information
  - Messed-up situational awareness, self separation, and collision avoidance
  - Ground controller and automation system confusion
  - Crippled ATC guidance when air and ground pictures are different
  - Can pilot still fly the way he/she prefers and arrive on time at planned destination? Can anyone depart knowing there is spoofing? Is it safe to fly at all?
- What are the planned ways to detect and handle spoofing (potentially in large quantity) and manage all automation systems?
  - Not very clear. Are we prepared?
- What may be the cost if such havoc is allowed to happen?
  - To operators, passengers, government, and society in general?

OUR TWO CENTS…

- A more prudent approach to APNT CONOPS may need to consider both ***jamming*** and ***spoofing*** threats
- We propose a new terminology, ***Resilient PBN*** *(R-PBN),* for ***NextGEN APNT*** to distinguish it from the currently-available DME/VOR/ILS based APNT concept
- ***R-PBN*** should ensure the safety and efficiency of NextGEN PBN during intermittent and prolonged jamming and spoofing events in a seamless, continuous, and unlimited manner.



SAAB TECHNOLOGIES SAAB 75 YEARS OF DEFENCE AND SECURITY

SAABSENSIS.COM